

Ahmed Emad Eldeen Abdelmoneam

LinkedIn: <https://www.linkedin.com/in/0x3omda/>

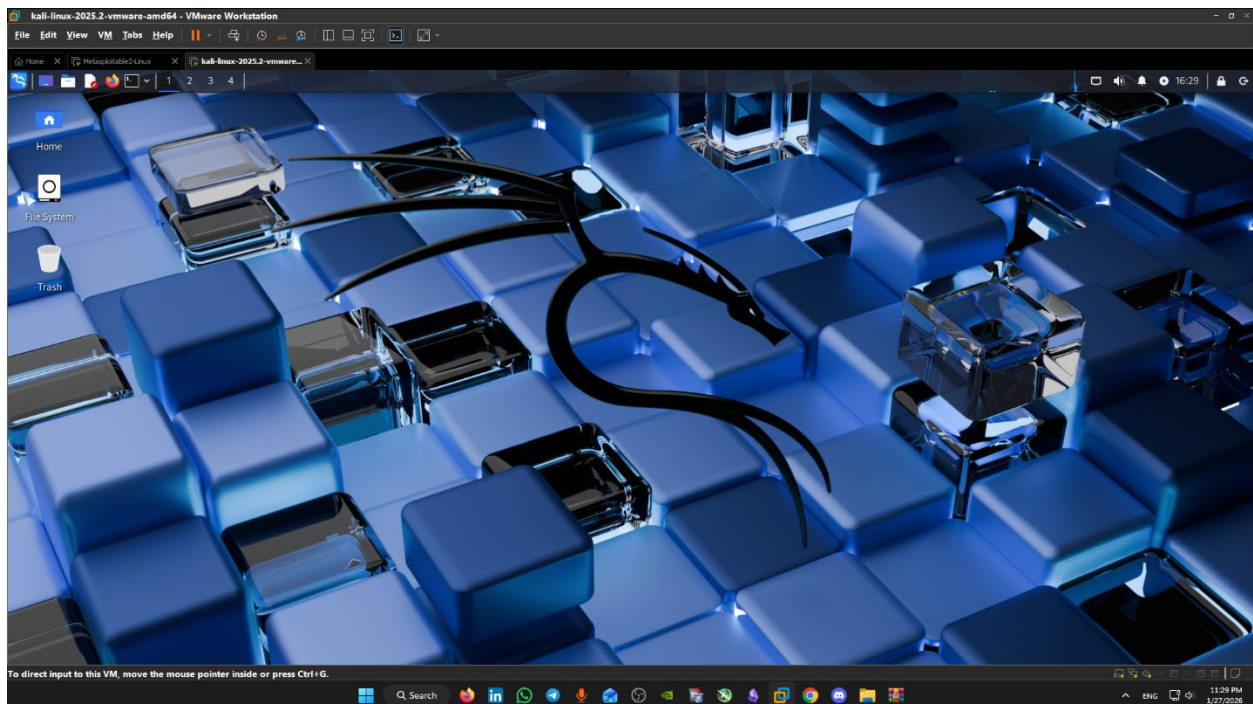
Portfolio : <https://eng-ahmed-emad.github.io/AhmedEmad-Dev/>

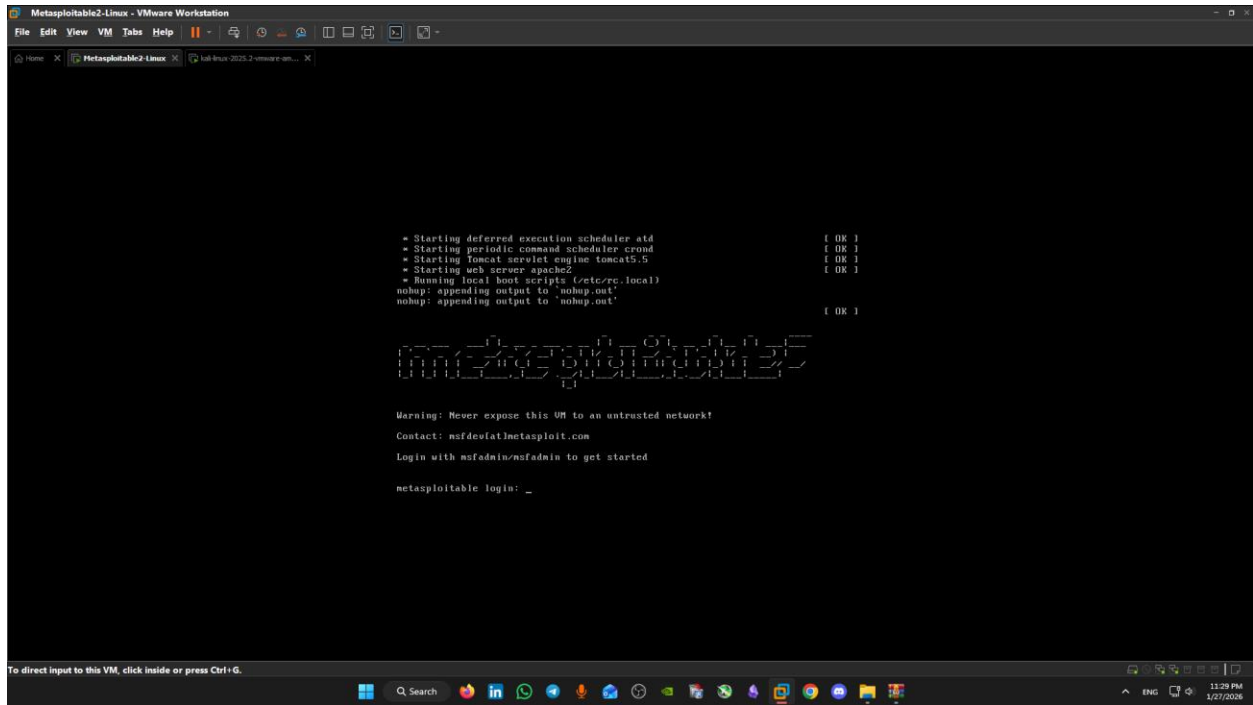
PostgreSQL Port : 5432

PostgreSQL is an open-source, object-relational database management system (ORDBMS) used to store and manage structured data.

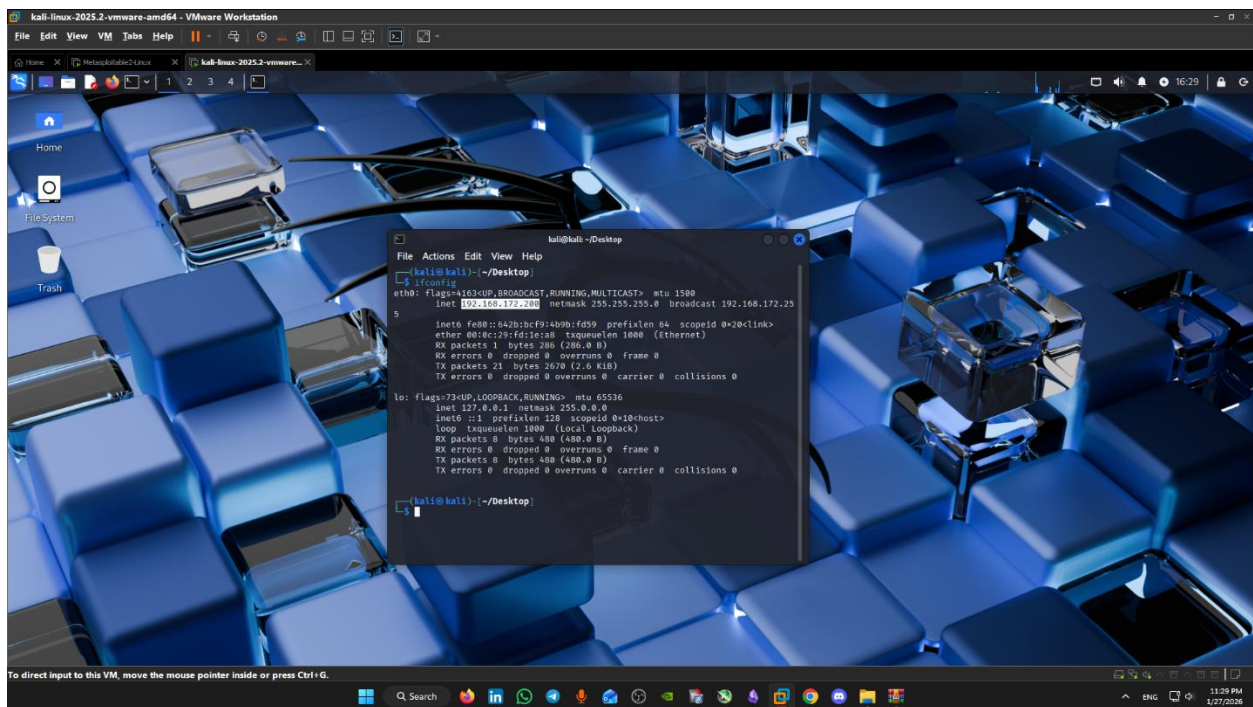
It is widely adopted in enterprise and web applications due to its reliability, extensibility, and strong support for SQL standards.

First I Installed Kali Linux And Metasploitable Machines





Second : I used **ifconfig** to know my ip and subnet (Target IP located: 192.168.172.129):



I Found Out It Was 192.168.172.0/24 so I used a simple Nmap Command On whole network and found out that machine has IP address of 192.168.172.129/24

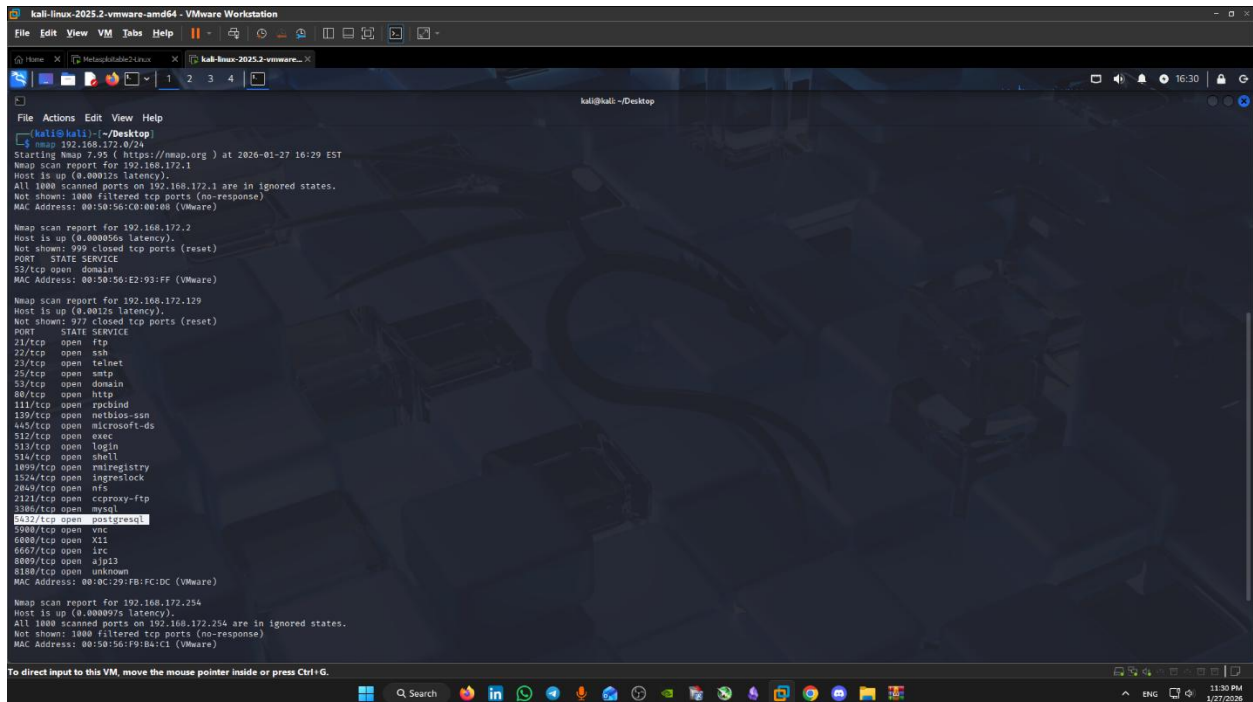
3. Port Scanning

Command:

Bash

```
nmap -p- 192.168.172.129
```

→ Port 5432 found open → service: postgresql



```
kali@kali:~/Desktop
└─$ nmap 192.168.172.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-27 16:29 EST
Nmap scan report for 192.168.172.1
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.172.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:80:108 (VMware)

Nmap scan report for 192.168.172.2
Host is up (0.000066s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
52/tcp    open  domain
MAC Address: 00:50:56:E2:93:FF (VMware)

Nmap scan report for 192.168.172.129
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
52/tcp    open  domain
80/tcp    open  http
111/tcp   open  rcbind
139/tcp   open  smbios-ssn
443/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3180/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x21
6067/tcp  open  irc
8080/tcp  open  ajp13
1180/tcp  open  unknown
MAC Address: 00:0C:29:FB:FC:DC (VMware)

Nmap scan report for 192.168.172.254
Host is up (0.000097s latency).
All 1000 scanned ports on 192.168.172.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F9:B4:C1 (VMware)
```

I found that the port I am curious about is open which is port **5432**

Fourth : I wanted to know the version so I used -A option which

4. Detailed Service & Version Fingerprinting

Command:

Bash

```
nmap -A -p 5432 192.168.172.129
```

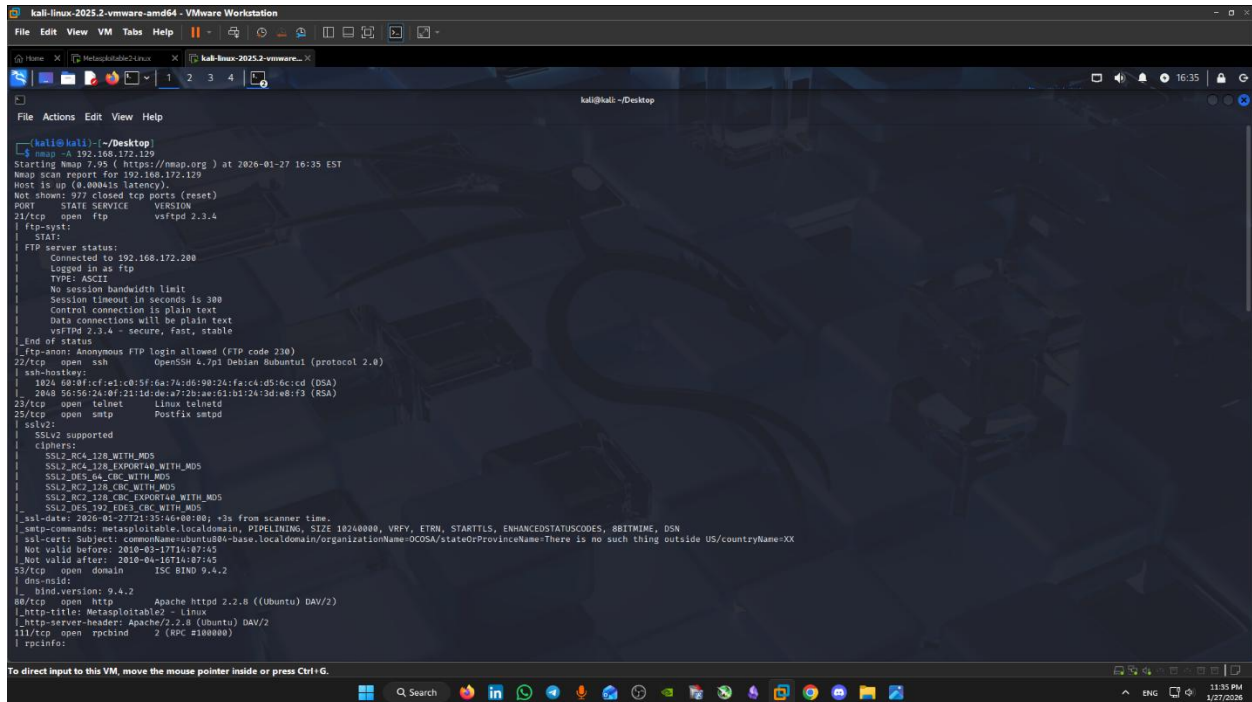
Result:

text

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

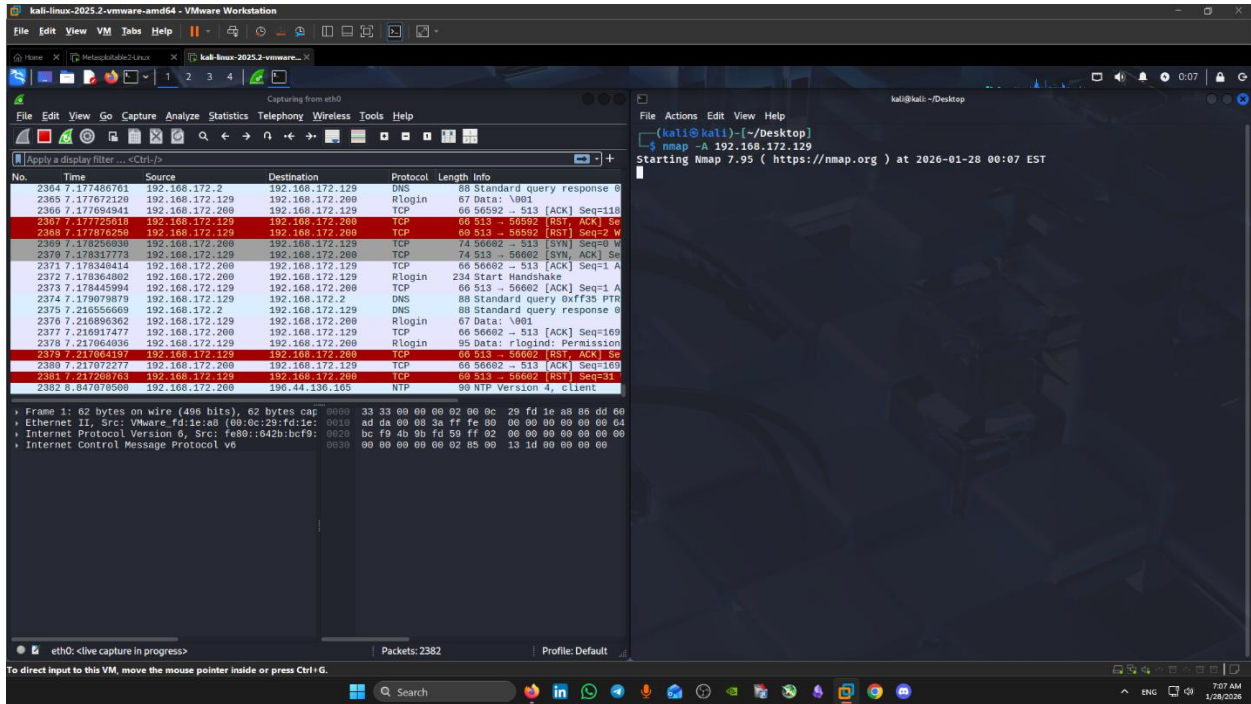
Confirmed version: **PostgreSQL 8.3.0 – 8.3.7**

enables **aggressive scan mode**, which combines **OS detection**, **version detection**, **default scripts (NSE)**, and **traceroute** in a single scan.



```
kali@kali:~$ nmap -A 192.168.172.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-27 16:35 EST
Nmap scan report for 192.168.172.129
Host is up (0.0000s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STATE:
|_FTP server status:
|_   Connected to 192.168.172.208
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsftpd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 330)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 66:0f:cfc1:d5f5:6a:7a:d5:98:26:fa:6b:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:11:1d:0e:a7:2b:a6:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RSA4096_WITH_MD5
|_  SSL2_RSA4096_WITH_MD5_EXPORT40_WITH_MD5
|_  SSL2_RSA1024_WITH_MD5
|_  SSL2_RSA1024_EXPORT40_WITH_MD5
|_ssl-date: 2026-01-27T21:35:46+08:00; +3s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu@base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-10T11:07:45
53/tcp    open  domain     ISC BIND 9.4.2
|_dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploit4e2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind    2 (port 11098880)
|_rpcinfo:
```

And this is how nmap scan appears in **Wireshark** which help me improve my **Analysis Skills (Educational)** 😊



I found out that the version is **PostgreSQL DB 8.3.0 - 8.3.7**

And I found 3 CVE's in NVD and 1 in Exploit DB (CVE-2012-0868)

- **CVE-2012-0868**
- **CVE-2012-2655**
- **CVE-2010-4015**
-

NVD Report : <https://nvd.nist.gov/vuln/detail/cve-2012-0868>

VULNERABILITIES

CVE-2012-0868 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:



NIST: NVD

Base Score: 6.8 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P)

QUICK INFO

CVE Dictionary Entry:

CVE-2012-0868

NVD Published Date:

07/18/2012

NVD Last Modified:

04/10/2025

Source:

Red Hat, Inc.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URI

Source(s)

Top(s)

6. Vulnerability Research

Searched National Vulnerability Database (NVD) and Exploit-DB for CVEs affecting PostgreSQL 8.3.x:

CVE ID	CVSS v2 Score	Vulnerability Type	Impact	Reference
CVE-2012-0868	6.8 (Medium)	SQL Injection via CRLF in pg_dump/restore	Arbitrary SQL execution during restore from crafted backup	https://nvd.nist.gov/vuln/detail/CVE-2012-0868
CVE-2012-2655	4.0 (Medium)	Denial of Service via SECURITY DEFINER functions	Authenticated users can crash the PostgreSQL server	NVD / PostgreSQL notes
CVE-2010-4015	6.5 (Medium)	Buffer overflow in intarray module (gettoken)	DoS + potential remote code execution (authenticated users)	NVD

VULNERABILITIES

CVE-2012-2655 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated users to cause a denial of service (server crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD

Base Score: 4.0 MEDIUM

Vector: (AV:N/AC:L/Au:S/C:N/I:N/A:P)

QUICK INFO

CVE Dictionary Entry:

CVE-2012-2655

NVD Published Date:

07/18/2012

NVD Last Modified:

04/10/2025

Source:

Red Hat, Inc.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed,

VULNERABILITIES

CVE-2010-4015 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Buffer overflow in the gettoken function in contrib/intarray/_int_bool.c in the intarray module in PostgreSQL 9.0.x before 9.0.3, 8.4.x before 8.4.7, 8.3.x before 8.3.14, and 8.2.x before 8.2.20 allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via integers with a large number of digits to unspecified functions.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD

Base Score: 6.5 MEDIUM

Vector: (AV:N/AC:L/Au:S/C:P/I:P/A:P)

QUICK INFO

CVE Dictionary Entry:

CVE-2010-4015

NVD Published Date:

02/01/2011

NVD Last Modified:

04/10/2025

Source:

Apple Inc.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this

ExploitDB : <https://www.exploit-db.com/exploits/7855>

The screenshot shows the ExploitDB interface for a PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution exploit. The page features a dark blue header with the Exploit Database logo and navigation icons. A vertical orange sidebar on the left contains various utility icons. The main content area is white and displays the exploit details in a structured layout. At the top, the title 'PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution' is highlighted in blue. Below the title, there are three white boxes containing key information: EDB-ID (7855), CVE (N/A), Author (BERNARDO DAMELE), Type (LOCAL), Platform (LINUX), and Date (2009-01-25). A green checkmark indicates 'EDB Verified', and a download icon is present for the exploit. The 'Vulnerable App' field is currently empty. Below this information, a light gray box contains the exploit description and references. The description reads: 'PostgreSQL UDF for command execution'. Two references are listed: [1] <http://bernardodamele.blogspot.com/2009/01/command-execution-with-postgresql-udf.html> and [2] https://svn.sqlmap.org/sqlmap/trunk/sqlmap/extra/postgresqludfsys/lib_postgresqludf_sys_0.0.1.tar.gz. A mirror link is also provided: <https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/7855.tar.gz> (2009-lib_postgresqludf_sys_0.0.1.tar.gz). A comment from 'milw0rn.com' dated '2009-01-25' is also visible. At the bottom of the page, there are navigation tabs for 'Databases', 'Links', 'Sites', and 'Solutions'.

Vulnerability Summary

CVE ID: CVE-2012-0868

Severity: Medium (CVSS v2.0: 6.8)

Type: SQL Injection via CRLF/Newline injection during backup restore

Impact: Execution of arbitrary SQL commands during the database restore process

CVE ID: CVE-2012-2655

Severity: Medium (CVSS v2.0: 4.0)

Type: Denial of Service due to improper handling of SECURITY DEFINER/SET in procedural language call handlers

Impact: Remote authenticated users can crash the PostgreSQL server, causing a denial of service

CVE ID: CVE-2010-4015

Severity: Medium (CVSS v2.0: 6.5)

Type: Buffer overflow in PostgreSQL intarray module (gettoken function)

Impact: Remote authenticated users can cause a denial of service and potentially execute arbitrary code

Additional Exploit Reference: Exploit-DB 7855 – PostgreSQL UDF code execution <https://www.exploit-db.com/exploits/7855>

Critical Note: PostgreSQL 8.3 branch is **End-of-Life** since 2013 → no security updates → highly vulnerable when network-accessible.

Conclusion

- Successfully identified PostgreSQL 8.3.0–8.3.7 on port 5432.
- Located multiple medium-severity vulnerabilities exploitable due to outdated software.
- Demonstrated complete reconnaissance workflow: network discovery → port scan → version detection → vulnerability enumeration.

-

Tools & Resources Used

- ifconfig
- Nmap (-sn, -p-, -A)
- Wireshark
- NVD
- Exploit-DB

-

Prepared by: Ahmed Emad Eldeen Abdelmoneam

Benha – January 2026